

2

# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

### COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 08 OCT. 2003

Pour le Directeur général de l'Institut national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS  
CONFORMÉMENT À LA  
RÈGLE 17.1.a) OU b)

BEST AVAILABLE COPY

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersbourg  
75800 PARIS cedex 08  
Téléphone : 33 (0)1 53 04 53 04  
Télécopie : 33 (0)1 53 04 45 23  
www.inpi.fr



INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08  
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

# CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre V

08540 W / 010201  
N° 11354\*02

## REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 010201

REMISSION DES PIÈCES		Réservé à l'INPI	
LIEU 18 DEC 2002 75 INPI PARIS		NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSEÉE	
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI		CABINET PLASSERAUD 84, rue d'Amsterdam 75440 PARIS CEDEX 09	
Vos références pour ce dossier (facultatif) BLO/FC-BFF020388			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		<input checked="" type="checkbox"/> Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale ou demande de certificat d'utilité initiale		N°	Date
Transformation d'une demande de brevet européen Demande de brevet initiale		N°	Date
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
PROCEDE DE COMMUNICATION ENTRE DEUX UNITES, ET TERMINAL METTANT EN OEUVRE LE PROCEDE			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date <input type="text"/> N° Pays ou organisation Date <input type="text"/> N° Pays ou organisation Date <input type="text"/> N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		FRANCE TELECOM	
Prénoms		Société Anonyme	
Forme juridique		380129866	
N° SIREN			
Code APE-NAF			
Domicile ou siège	Rue	6, place d'Alleray 75015 PARIS	
	Code postal et ville	<input type="text"/>	
	Pays	FRANCE Française	
Nationalité		N° de télécopie (facultatif)	
N° de téléphone (facultatif)		<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»	
Adresse électronique (facultatif)		Remplir impérativement la 2 <sup>me</sup> page	

**BREVET D'INVENTION  
CERTIFICAT D'UTILITÉ**

**REQUÊTE EN DÉLIVRANCE**  
page 2/2

**BR2**

Réserve à l'INPI

REMISE DES PIÈCES

DATE

LEU 18 DEC 2002

75 INPI PARIS

N° D'ENREGISTREMENT

NATIONAL ATTRIBUÉ PAR L'INPI

0216092

DB 540 W / 01CSN

Vos références pour ce dossier :  
(facultatif)

BLO/FC-BFF020388

**6 MANDATAIRE (s'il y a lieu)**

Nom

Prénom

Cabinet ou Société

N° de pouvoir permanent et/ou  
de lien contractuel

Rue

Cabinet PLASSERAUD

Adresse

Code postal et ville

84, rue d'Amsterdam

75009 PARIS

Pays

N° de téléphone (facultatif)

N° de télécopie (facultatif)

Adresse électronique (facultatif)

**7 INVENTEUR (S)**

Les inventeurs sont nécessairement des personnes physiques

Oui

Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)

**8 RAPPORT DE RECHERCHE**

Uniquement pour une demande de brevet (y compris division et transformation)

Établissement immédiat  
ou établissement différé

Paiement échelonné de la redevance  
(en deux versements)

Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt

Oui

Non

**9 RÉDUCTION DU TAUX  
DES REDEVANCES**

Uniquement pour les personnes physiques

Requise pour la première fois pour cette invention (joindre un avis de non-imposition)

Obtenu antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG

Si vous avez utilisé l'imprimé « Suite »,  
indiquez le nombre de pages jointes

**10 SIGNATURE DU DEMANDEUR  
OU DU MANDATAIRE**

(Nom et qualité du signataire)

Bertrand LOISEL

CPI n° 940311

**VISA DE LA PRÉFECTURE  
OU DE L'INPI**

**PROCEDE DE COMMUNICATION ENTRE DEUX UNITES,**  
**ET TERMINAL METTANT EN ŒUVRE LE PROCEDE**

La présente invention concerne les terminaux informatiques permettant des activités de type navigation sur réseau et offrant aux utilisateurs la 5 possibilité d'installer des applications.

De tels terminaux peuvent notamment être des téléphones utilisant le protocole d'application sans fil (WAP, "wireless application protocol"), des ordinateurs de bureau, des ordinateurs portables ou des assistants numériques personnels (PDA, "personal digital assistant"). Ils ont en commun la 10 caractéristique d'être reliés à un réseau de données numérique, qui dans beaucoup de cas pratiques est un réseau fonctionnant selon le protocole IP ("Internet protocol"), notamment l'Internet.

Dans le cas d'un terminal "fermé" (exemple: un Minitel), les 15 applications présentes sur le terminal sont connues et ne peuvent pas être changées au cours de la vie du terminal.

L'ouverture d'un terminal fait référence à la possibilité offerte à l'utilisateur d'installer, et souvent de télécharger, de nouvelles applications destinées à être exécutées par le terminal lui-même. Des exemples de terminaux "ouverts", intégrant cette possibilité, sont:

- 20     • les téléphones à téléchargement d'applications, par exemple de type Java MIDP ("Mobile Information Device Profile", Sun Microsystems, Inc.);
- les navigateurs possédant des fonctionnalités dites de scripting, par exemple de type WMLScript (voir "WAP WMLScript Language Specification", version 1.1, WAP Forum, novembre 2001) ou ECMAScript 25 (aussi appelé JavaScript, voir "ECMAScript Language Specification", Standard ECMA-262, 3<sup>e</sup> édition, décembre 1999), ou accueillant des applets;
- la plupart des PDA, fonctionnant sous les systèmes d'exploitation PalmOS, WindowsCE, Symbian etc.;
- 30     • les ordinateurs de bureau ou portables.

Les terminaux "semi-ouverts" sont les terminaux ouverts dont certaines fonctionnalités ne sont pas directement accessibles aux applications installées par l'utilisateur ou téléchargées. Par exemple, dans un terminal dont la seule "ouverture" est ECMAScript, les applications téléchargées ne peuvent pas accéder à toutes les fonctionnalités du réseau (par exemple, émettre des paquets IP n'obéissant pas aux formats des protocoles de transport les plus courants, à savoir TCP ("transmission control protocol") ou UDP ("user datagram protocol")). Ces fonctionnalités peuvent être accessibles de façon indirecte et contrôlée. Par exemple, une fonction ECMAScript peut commander le chargement d'une page via HTTP ("hypertext transfer protocol"), ce qui utilise le réseau mais d'une façon contrôlée.

Dans des terminaux "semi-ouverts", il y a coexistence:

- d'applications considérées comme "de confiance", par exemple parce qu'elles ont été installées en usine par le fabricant du terminal, ou bien du fait de la garantie procurée par des moyens tels que la signature électronique de l'application etc.;
- et d'autres applications qui peuvent être installées sur le terminal par l'utilisateur lui-même, à son libre choix, mais n'accèdent pas aux mêmes droits que les applications de confiance.

Les terminaux "complètement ouverts", par opposition, sont les terminaux ouverts dans lesquels toutes les fonctionnalités sont accessibles aux applications téléchargées. La notion d'ouverture d'un terminal dépend dans une large mesure du contexte dans lequel on se place. Par exemple, différentes couches du modèle OSI (lien / réseau / session / transport / ...) peuvent avoir différents degrés d'ouverture.

On s'intéresse ici aux fonctionnalités observables à distance, depuis un serveur, c'est-à-dire aux fonctionnalités de réseau. Dans ce cadre, le caractère "semi-ouvert" d'un terminal implique généralement que des droits d'exécution observables à distance, accessibles aux applications de confiance, ne sont pas accessibles aux applications sans confiance (par exemple, le droit d'émettre des requêtes autres que HTTP sur un réseau IP). Ceci permet à un serveur de

distinguer, parmi les requêtes qui lui arrivent, celles qui proviennent d'applications de confiance et celles qui proviennent d'autres applications. Il peut en particulier distinguer les requêtes provenant d'applications téléchargées des requêtes provenant d'applications présentes dès l'origine 5 dans le terminal.

Dans les terminaux ouverts, il faut tenir compte de la possibilité qu'un programme se comporte de façon trompeuse vis-à-vis de l'utilisateur (cheval de Troie). Ainsi, rien ne peut garantir à un serveur qu'une requête provient bien de l'utilisateur, et non d'un programme ayant simulé l'accord de l'utilisateur au 10 niveau du réseau. Ce risque ruine la confiance que le serveur peut avoir dans les données qu'il reçoit d'un client. L'hypothèse selon laquelle les requêtes adressées au serveur reflètent les actions de l'utilisateur n'est pas raisonnable si un cheval de Troie a la possibilité de les envoyer à la place de l'utilisateur.

On fera donc dans la suite une distinction entre les applications 15 présentes sur le terminal:

- applications de confiance: le serveur est prêt à faire l'hypothèse que ces applications ne sont pas des chevaux de Troie. Par exemple, le navigateur WAP d'un téléphone WAP peut constituer une application de confiance. Un autre exemple peut être une application Java MIDP 20 téléchargée avec signature;
- applications sans confiance: le serveur considère que ces applications peuvent être des chevaux de Troie. Par exemple, des applications Java MIDP téléchargées sans signature sur un terminal peuvent être des applications sans confiance.

25 La réponse classique au risque de cheval de Troie est de limiter les capacités des applications sans confiance.

La limitation de l'émission des trames depuis les terminaux semi-ouverts se fait généralement de façon extrêmement stricte. Seules les applications système (fournies avec le système d'exploitation du terminal) sont 30 autorisées à émettre certaines trames.

Il devient donc impossible à une application téléchargée (avec ou sans confiance) d'émettre des trames vers un serveur, même si cette application dispose par ailleurs de moyens d'obtenir la confiance du serveur du fait du contenu des trames qu'elle émet (exemple: émission de données signées) ou 5 du fait de ses caractéristiques (exemple: signature associée à son contenu).

Un but de la présente invention est d'offrir une différence de capacité d'envoi de requêtes d'un nouveau type entre applications "de confiance" et applications "sans confiance", qui soit flexible pour les applications et puisse néanmoins être identifiée par le serveur destinataire. La notion de confiance 10 peut s'appuyer sur des critères variés (signature, type d'échange, URL depuis laquelle l'application a été téléchargée, etc.).

L'invention propose ainsi un procédé de communication entre une première unité et une seconde unité par l'intermédiaire d'un réseau de télécommunication, dans lequel la première unité comporte des applications 15 appartenant respectivement à une première famille et à une seconde famille présentant a priori un degré de confiance plus faible que la première famille. Selon un aspect de l'invention, on constraint chaque requête issue d'une application de la seconde famille, émise sur le réseau à destination de la seconde unité, à inclure un marquage associé à la seconde famille 20 d'applications. Selon un autre aspect de l'invention, on constraint chaque requête issue d'une application de la seconde famille, émise sur le réseau à destination de la seconde unité, à ne pas inclure un marquage associé à la première famille, ledit marquage étant inclus dans certaines au moins des requêtes émises sur le réseau et issues d'applications de la première famille. 25 L'invention propose aussi un terminal de communication, comprenant des moyens de mise en œuvre d'un tel procédé en tant que première unité.

Le procédé permet à certaines applications particulières ("de confiance") s'exécutant dans la première unité d'émettre des trames à l'attention d'une seconde unité, généralement un serveur distant, avec la 30 garantie pour cette seconde unité de l'origine fiable de ces trames. L'inclusion obligatoire du marquage pour les applications a priori sans confiance de la seconde famille (ou symétriquement son interdiction) distingue, à l'émission,

les trames émises par ces applications a priori sans confiance par rapport à celles émises par des applications de confiance. Ceci permet au serveur de faire le tri entre les requêtes acceptables, en lesquelles il a confiance, et celles qu'il doit rejeter.

5        Il convient que le marquage appliqué soit complètement "étanche", c'est-à-dire qu'il ne soit pas possible pour une application a priori sans confiance de court-circuiter les contrôles effectués à un certain niveau (par exemple: fonctions de requêtes HTTP), en attaquant les couches plus basses (par exemple: requête d'une connexion TCP).

10       Dans une réalisation du procédé, on constraint le marquage, inclus dans une requête émise sur le réseau et issue d'une application de la seconde famille, à inclure une indication de la nature et/ou de l'origine de ladite application de la seconde famille. Cette indication consiste par exemple en des données relatives à la certification de la signature d'une application signée, ou 15       encore à l'adresse de téléchargement d'une application téléchargée par l'intermédiaire du réseau. Elle peut être utilisée par l'unité distante pour évaluer si elle peut faire confiance à l'application qui ne pouvait a priori qu'être jugée sans confiance par la première unité.

20       Grâce au procédé, des terminaux supportant le téléchargement des applications peuvent échanger des données en toute confiance avec un serveur, malgré les risques inhérents à ces capacités de téléchargement ("ouverture" du terminal). Le procédé procure ainsi une protection simple et efficace contre les chevaux de Troie.

25       D'autres particularités et avantages de la présente invention apparaîtront dans la description ci-après d'exemples de réalisation non limitatifs, en référence au dessin annexé, dans lequel la figure unique est un schéma d'un système mettant en œuvre l'invention.

30       On cherche à permettre à une unité distante telle qu'un serveur 1 d'obtenir de façon sûre et souple la confiance dans des requêtes reçues sur un réseau de télécommunication R en provenance d'un terminal semi-ouvert 2. Ce terminal héberge d'une part des applications de confiance 3, comme par

exemple un navigateur web, et d'autre part des applications a priori sans confiance 4, notamment des applications que l'utilisateur du terminal a téléchargées par l'intermédiaire du réseau R.

5 Les applications a priori sans confiance 4 sont contraintes quant aux trames ou requêtes qu'elles peuvent émettre sur le réseau R, ce qui, dans le schéma, est symbolisé par une couche de contrôle 5 faisant partie des ressources 6 d'accès au réseau dont est équipé le terminal 2.

10 La couche de contrôle 5 vérifie que certaines propriétés sont remplies par les trames émises par les applications a priori sans confiance 4. Si ces propriétés sont remplies, la couche de contrôle laisse passer les trames. Sinon, elle peut soit ne pas les laisser passer vers le réseau R et en prévenir l'application 4 qui les a émises, soit modifier les trames pour les conformer aux contraintes des applications a priori sans confiance. Dans ce dernier cas, la trame perd sa crédibilité aux yeux du serveur 1, qui pourra ne pas l'exploiter.

15 Les contraintes précitées se rapportent à la présence ou non d'un marquage spécifique dans les requêtes émises sur le réseau R depuis certaines des applications.

20 Dans un premier mode de réalisation de l'invention, la couche de contrôle 5 impose aux requêtes issues des applications a priori sans confiance 4 d'inclure un marquage associé à cette famille d'applications. Une application de confiance 3 accède à des fonctionnalités qui lui permettent de contourner la couche de contrôle 5 et d'émettre des requêtes non marquées. En revanche, les ressources 6 d'accès au réseau ne mettent pas ces fonctionnalités à disposition des applications a priori sans confiance 4.

25 Dans un exemple illustrant ce premier mode de réalisation, le terminal 2 (par exemple un téléphone mobile) dispose d'une machine virtuelle Java, pouvant correspondre au module 6 sur la figure. La machine virtuelle permet d'exécuter des applications téléchargées écrites dans le langage de programmation Java mis au point par la société Sun Microsystems, Inc. Toutes 30 les instructions du langage Java sont exécutées par la machine virtuelle, qui fait appel aux fonctions système après un certain contrôle. Pour les

applications Java, on est bien dans un environnement semi-ouvert puisqu'il n'y a pas d'appel sans contrôle aux fonctions système. Ce terminal 2 n'est capable de télécharger que du code Java, aucun autre type d'application ne pouvant y être installé par l'utilisateur.

5           L'application a priori sans confiance 4 est alors écrite en langage Java.

Dans cet exemple, les protocoles mis en jeu pour les échanges du terminal 2 sur le réseau R sont les protocoles HTTP (RFC 1945 ("Request For Comments"), publiée en mai 1996 par l'IETF ("Internet Engineering Task Force")), TCP (RFC 793, IETF, septembre 1981) et IP (RFC 791, IETF, 10 septembre 1981).

Le service est hébergé par un serveur HTTP 1 qui stocke du contenu appartenant à l'utilisateur. Il doit s'assurer du fait qu'une requête (demandant par exemple l'effacement de tous les fichiers) provient bien de l'utilisateur, et non d'un programme Java mal intentionné. Ce service est bien entendu un exemple, n'importe quel autre service pouvant être faire appel à cette technique (commerce électronique, publication de documents, messagerie, etc.).

Le marquage peut être inclus dans le champ d'en-tête "User-Agent" des requêtes HTTP (cf. section 10.15 de la RFC 1945 précitée). Il consiste en 20 une chaîne spécifique telle que "Application sans confiance: VM Java 1.2" qui indique par sa présence que la requête n'est pas en provenance d'une application a priori de confiance. Cette chaîne peut être déjà présente dans la requête produite par l'application 4, auquel cas la couche de contrôle 5 de la machine virtuelle 6 se contente de vérifier sa présence. Sinon, 25 cette couche 5 l'insère pour que la requête soit convenablement marquée.

L'étanchéité du marquage appliqué par la machine virtuelle 6 résulte de ce qu'il n'est pas possible à une application a priori sans confiance 4 d'émettre sur le réseau R des requêtes HTTP ne contenant pas cette chaîne spécifique. En particulier, l'application 4 ne peut pas avoir accès au réseau R 30 en se branchant sur une couche protocolaire plus basse que HTTP, notamment aux sockets TCP. Le marquage est implémenté directement dans

la machine virtuelle 6 dans laquelle l'application a priori sans confiance est obligée de s'exécuter et qu'elle ne peut éviter d'aucune manière.

Le serveur 1 peut ainsi trier, parmi les requêtes qui lui arrivent, celles qui proviennent d'applications a priori sans confiance 4 et celles qui 5 proviennent d'applications de confiance 3 telles qu'un navigateur web.

Il existe des applications qui ne sont de confiance que pour certains sites. Par exemple, une applet Java est généralement considérée comme de confiance par le site depuis lequel elle a été téléchargée, mais non par d'autres sites. Le marquage ne sera donc pas toujours nécessaire dans les requêtes 10 destinées à ce site de téléchargement. En d'autres termes, la machine virtuelle 6 peut imposer le marquage aux requêtes issues d'une telle applet et émises vers un site autre que celui d'où elle a été téléchargée et laisser l'applet libre d'inclure ou non le marquage dans les requêtes qu'elle émet vers son site d'origine. Une autre possibilité est d'imposer le marquage à toute requête 15 émise par une telle applet, quelle qu'en soit la destination.

Une alternative ou un complément au marquage des requêtes sans confiance peut être l'interdiction de certaines de ces requêtes. Par exemple, pour des applications sans confiance téléchargées depuis un serveur donné, les requêtes directes à destination de serveurs différents pourraient être 20 interdites. Les requêtes à destination du serveur d'origine resteraient possibles, avec le marquage.

Dans une réalisation avantageuse, on adjoint obligatoirement au marquage une indication de la nature et/ou de l'origine de l'application a priori sans confiance 4 dont elle est issue.

25 Cette application a priori sans confiance 4 peut être signée. Les requêtes qui en proviennent seront alors marquées avec un en-tête contenant au moins l'un des éléments suivants, susceptibles de fonder la confiance du serveur distant dans cette application:

- le certificat du signataire de l'application, ou un condensé de ce certificat;

- le certificat de la chaîne de certification d'où le certificat du signataire de l'application est issu, ou un condensé de ce certificat;
- une chaîne spécialement incluse dans le code de l'application à cet effet;
- un élément variable identifiant l'application de manière dynamique.

5           Une telle réalisation de l'invention est notamment applicable dans le cas d'une application Java signée par un certificat.

          Dans ce cas, la machine virtuelle 6 doit vérifier la signature de l'application Java avant l'émission des requêtes. En pratique, cette vérification a lieu avant l'exécution de l'application 4.

10           Le marquage peut alors consister en l'ajout d'une chaîne spécifique dans l'en-tête HTTP, comme par exemple: "Contenu de confiance - Application signée par <C>" où <C> est la valeur du certificat du signataire de l'application, ou un condensé de celui-ci. Cet en-tête indique par sa présence que la requête est en provenance directe d'un utilisateur, et a été 15 créée par un logiciel de provenance connue.

          De cette façon, si le serveur 1 accorde sa confiance au détenteur des clefs privées associées au certificat <C>, le serveur est garanti que les requêtes marquées de cet en-tête spécifique correspondent bien à un accord effectif de l'utilisateur. La contrainte de marquage évite que l'application puisse, 20 auprès du serveur, se réclamer d'un signataire autre que le signataire réel.

          Dans le cas des applet Java téléchargées, la machine virtuelle 6 est capable d'identifier l'adresse de téléchargement de l'application. Elle peut ainsi contraindre la requête issue d'une telle applet, a priori sans confiance, d'inclure son adresse de téléchargement ou des données qui dépendent de cette 25 adresse.

          Dans un autre mode de réalisation de l'invention, la syntaxe du marquage est inversée: la couche de contrôle 5 impose aux requêtes issues des applications a priori sans confiance 4 de ne pas inclure un marquage spécifique aux applications de confiance 3.

Pour se manifester comme étant de confiance pour un serveur 1, une application 3 inclut alors le marquage dans la requête qu'elle lui adresse. La couche de contrôle 5 s'assure que ce marquage est absent de chaque requête issue d'une application a priori sans confiance 4, le caractère sans confiance 5 pouvant comme précédemment être apprécié en fonction du site destinataire de la requête. Si le marquage est présent dans une requête issue d'une application a priori sans confiance 4, la requête n'est pas émise telle quelle: le marquage est enlevé par la couche de contrôle 5 et celle-ci peut émettre ou non la requête "démarquée" sur le réseau R et prévenir ou non l'application 4.

10 La convention employée pour la syntaxe du marquage doit naturellement être commune au terminal et au serveur, et connue des deux avant la transaction.

## REVENDICATIONS

1. Procédé de communication entre une première unité (2) et une seconde unité (1) par l'intermédiaire d'un réseau de télécommunication (R), dans lequel la première unité comporte des applications (3, 4) appartenant respectivement à une première famille et à une seconde famille présentant a priori un degré de confiance plus faible que la première famille, caractérisé en ce qu'on constraint chaque requête issue d'une application (4) de la seconde famille, émise sur le réseau à destination de la seconde unité, à inclure un marquage associé à la seconde famille d'applications.
- 10 2. Procédé selon la revendication 1, dans lequel ledit marquage est inclus dans chaque requête émise sur le réseau (R) et issue d'une application de la seconde famille (4).
- 15 3. Procédé selon la revendication 1 ou 2, dans lequel on constraint le marquage, inclus dans une requête émise sur le réseau (R) et issue d'une application (4) de la seconde famille, à inclure une indication de la nature et/ou de l'origine de ladite application de la seconde famille.
- 20 4. Procédé selon la revendication 3, dans lequel, ladite application (4) de la seconde famille étant signée, on constraint le marquage, inclus dans les requêtes qui en sont issues, à inclure des données relatives à la certification de la signature.
- 25 5. Procédé selon la revendication 3 ou 4, dans lequel, ladite application (4) de la seconde famille ayant été téléchargée par l'intermédiaire du réseau (R) depuis une adresse de téléchargement, on constraint le marquage, inclus dans les requêtes qui en sont issues, à inclure des données relatives à l'adresse de téléchargement de l'application.

6. Procédé de communication entre une première unité (2) et une seconde unité (1) par l'intermédiaire d'un réseau de télécommunication (R), dans lequel la première unité comporte des applications (3, 4) appartenant respectivement à une première famille et à une seconde famille présentant a 5 priori un degré de confiance plus faible que la première famille, caractérisé en ce qu'on constraint chaque requête issue d'une application (4) de la seconde famille, émise sur le réseau à destination de la seconde unité, à ne pas inclure un marquage associé à la première famille, ledit marquage étant inclus dans certaines au moins des requêtes émises sur le réseau et issues d'applications 10 (3) de la première famille.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel la seconde unité (1) examine si le marquage est présent dans une requête reçue sur le réseau (R) depuis la première unité (2), pour évaluer un degré de confiance à attacher à ladite requête.

15 8. Procédé selon la revendication 7, dans lequel, lorsque le marquage est présent dans ladite requête, la seconde unité (1) examine en outre des données incluses dans ce marquage, pour évaluer un degré de confiance à attacher à ladite requête.

20 9. Procédé selon la revendication 8, dans lequel lesdites données examinées par la seconde unité (1) comprennent des données relatives à la certification d'une signature de l'application dont est issue la requête.

10. Procédé selon la revendication 8, dans lequel lesdites données examinées par la seconde unité (1) comprennent des données relatives à une adresse de téléchargement de l'application dont est issue la requête.

25 11. Procédé selon l'une quelconque des revendications précédentes, dans lequel les requêtes comprennent des requêtes HTTP, et le marquage est inséré dans les en-têtes des requêtes HTTP.

12. Procédé selon l'une quelconque des revendications précédentes, dans lequel la contrainte relative au marquage est contrôlée par une couche logicielle (5) appartenant à une machine virtuelle (6) dont est pourvue la première unité (2), les applications (4) de la seconde famille ne pouvant 5 accéder au réseau (R) qu'à travers la machine virtuelle et ladite couche logicielle.

13. Procédé selon la revendication 12, dans lequel la machine virtuelle (6) est une machine virtuelle Java.

14. Terminal de communication (2), comprenant des moyens de mise en 10 œuvre d'un procédé selon l'une quelconque des revendications précédentes en tant que première unité.

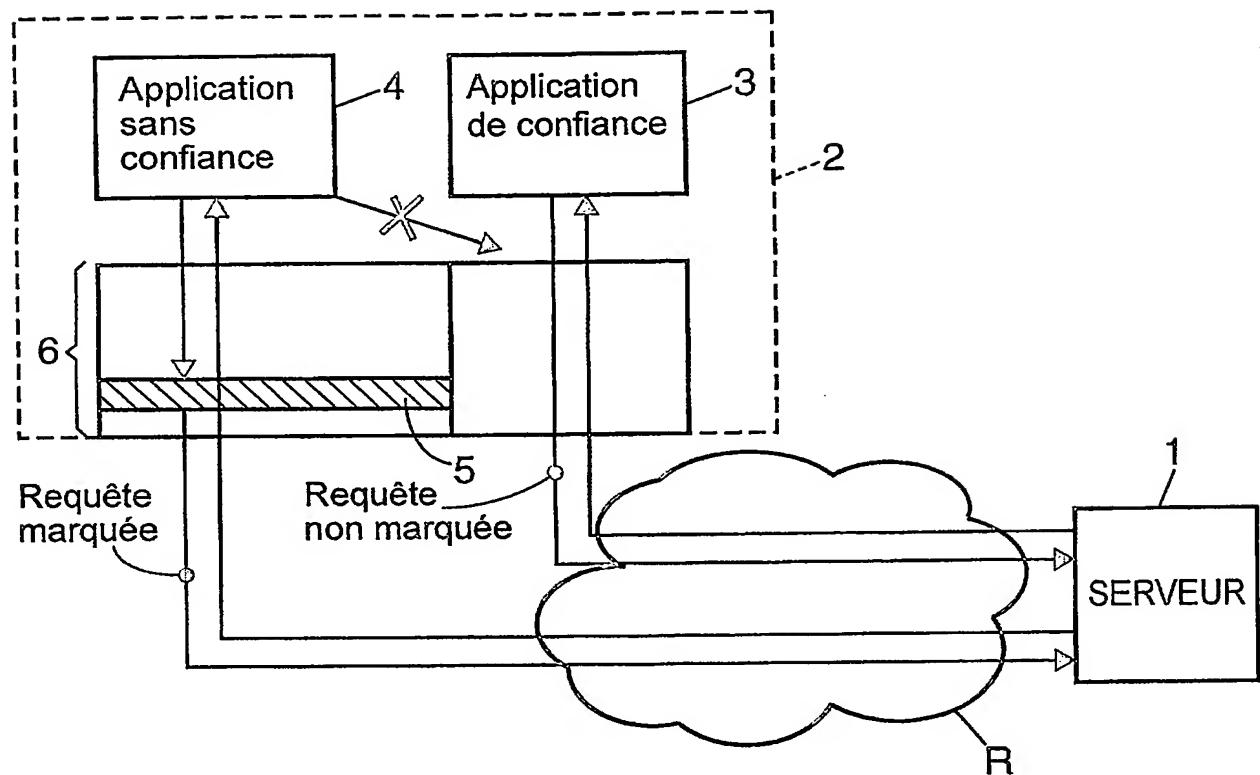


FIG. Unique

**CERTIFICAT D'UTILITÉ**

Code de la propriété intellectuelle - Livre VI

**DÉSIGNATION D'INVENTEUR(S)** Page N° 1/1

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 312 27/03/03

DÉPARTEMENT DES BREVETS

16 bis, rue de Saint Pétersbourg  
5800 Paris Cedex 08  
téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

Vos références pour ce dossier (facultatif)

N° D'ENREGISTREMENT NATIONAL

BLO/FC-BFF020388

0216072

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE COMMUNICATION ENTRE DEUX UNITES, ET TERMINAL METTANT EN OEUVRE LE PROCEDE

LE(S) DEMANDEUR(S) :

FRANCE TELECOM

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

<input checked="" type="checkbox"/> Nom	DE BOURSETTY Benoît		
Prénoms			
Adresse	Rue	3, rue des Volontaires	75015 PARIS
	Code postal et ville		FRANCE
Société d'appartenance (facultatif)			
<input checked="" type="checkbox"/> Nom	GRUSON Manuel		
Prénoms			
Adresse	Rue	14, Villa Dutry	75014 PARIS
	Code postal et ville		FRANCE
Société d'appartenance (facultatif)			
<input checked="" type="checkbox"/> Nom	MOUTON Dimitri		
Prénoms			
Adresse	Rue	11, rue Antoine Bourdelle	75015 PARIS
	Code postal et ville		FRANCE
Société d'appartenance (facultatif)			

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivie du nombre de pages.

DATE ET SIGNATURE(S)  
DU (DES) DEMANDEUR(S)

Le 18 décembre 2002

OU DU MANDATAIRE  
(Nom et qualité du signataire)

CABINET PLASSERAUD

Bertrand LOISEL

CPI n° 940311

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**